Questions for Mr. John Sherman
Chief Information Officer (CIO), Department of Defense

Questions from Chairman Gerald E. Connolly
Subcommittee on Government Operations

July 28, 2022, Hearing: "FITARA 14.0"

---

1. **In a letter to the Subcommittee prior to this hearing, you stated that the "Department of Defense (DoD) continues to believe its existing working capital fund (WCF) structure, policies, and processes meet the intent of the Modernizing Government Technology (MGT) Act." How does the DoD's existing WCF differ from that of an MGT Act fund, and how is it contributing to your agency's information technology (IT) modernization efforts?**

   The Department's current financial infrastructure contains multiple working capital funds and annual appropriations bills that provide the Department with a wide range of financial flexibilities, including transfer and reprogramming authorities, to manage our resources and mission throughout the year. The Defense-wide WCF, which is used by the Defense Information Systems Agency (DISA) as DoD's enterprise provider, meets the MGT Act's WCF intent.

2. **Earlier this month, the Government Accountability Office released a report on cloud computing that assessed the DoD's Workforce Planning and Software Application Modernization. The report found that the DoD had implemented 11of the 14 recommendations. What is the DoD doing to ensure the other three recommendations related to security, workforce, and procurement are implemented as well?**

   The Department appreciates GAO's extensive review and acknowledgement of the DoD CIO's efforts to address key cloud computing requirements in the areas of security, procurement, and workforce. The Department has addressed cloud computing requirements and developed an enterprise-wide application rationalization process. In our response to GAO, we acknowledge that we are continuing to do more work and are preparing a corrective action plan to address the areas of application rationalization, skills gap analysis, and technology business management framework.

3. **Further, in line with the report's recommendations, how does DoD plan to better track cloud spending and investments?**

   DoD requires that every cloud service offering is designated as a unique investment within the Department's IT and Cyberspace Activities (IT/CA) budget. This establishes the cloud funding required for the management and operation of those cloud services. In

addition, the IT/CA budget captures funding associated with the specific migration and hosting costs across the Department's IT systems and applications. DoD provides a Congressional Cloud report with each President's Budget submission to not only provide funding transparency, but also to highlight the Department's overall cloud strategy.

4. Where is DoD in its adoption of multi-cloud and has the Department developed a multi-cloud strategy?

In February 2022, DoD published the Department of Defense Software Modernization Strategy which replaced the 2018 DoD Cloud Strategy. The first goal of the strategy is to accelerate the DoD Enterprise Cloud Environment using a multi-cloud, multi-vendor approach. A key step is accelerating progress toward this goal will the Joint Warfighting Cloud Capability (JWCC). JWCC is a multiple award acquisition vehicle that will provide DoD a vehicle with direct access to multiple cloud service providers. The intent is to provide Military Services and DoD Components with access to cutting edge commercial cloud technologies that enable the Department to innovate at speed and exceed the capabilities of our near-peer competitors. JWCC is under active procurement with expected award at the end of 2022.

Questions for Mr. John Sherman
Chief Information Officer (CIO), Department of Defense

Questions from Ranking Member Jody Hice
Subcommittee on Government Operations

July 28, 2022, Hearing: "FITARA 14.0"

---

1. **The description accompanying the Scorecard category titled "Enhanced Transparency and Improved Risk Management" says, "FITARA requires OMB to publicize detailed information on federal IT investments and requires agency CIOs to categorize their major IT investments by risk." DoD scored 50 percent on this category.**
    a. **Please explain how DoD defines "risk" and a "major IT investment."**

    DoD defines risk as "potential future events or conditions that may have a negative effect on achieving program objectives for cost, schedule, and performance," and categorizes risk using two major considerations: likelihood and impact level. OMB CIO risk evaluation guidance states that a CIO evaluation should reflect the "assessment of the risk and the investment's ability to accomplish its goals." CIO risk rating values for the ITDB are based on OMB's five-point risk scale. OMB assigns "low" numbers to high risks. In reverse contrast, DoD risk models correlate "high" numbers to high risks. Thus, it is paramount to avoid translation errors from DoD risk models to OMB values.

    The DoD defines a major IT investment based on the following criteria (revised for the FY24 budget), which have been negotiated with OMB:

    - Defense business system (DBS) with a total investment greater than $250M across the Future Years Defense Program (FYDP)
    - Non-DBS with a total greater than $569M across the FYDP
    - IT investments designated by the DoD CIO as a major IT investment due to factors such as, but not limited to:
        - Importance to the mission or function of the government;
        - Significant program or policy implications;
        - High executive visibility;
        - High investment or other risk; or
        - Unusual funding mechanisms.
    - Programs on the major defense acquisition program (MDAP) list, which is managed by the Under Secretary of Defense for Acquisition and Technology, determined to be IT by the DoD CIO. The MDAP IT investments are required to submit a selected acquisition report (SAR). No business cases are required for MDAP IT investments since these investments submit SARs.

b. Does DoD's grade mean that 50 percent of its major IT investments are at risk? Please explain the significance of DOD's grade in this category.

Yes. Out of the 45 Major IT Investments (NSS and Non-NSS) that are rated for risk, 50% are rated at medium, risk (yellow) or moderate/high risk (red).

c. What percentage of DoD's entire IT investment portfolio is comprised of "major IT investments"?

Major investments account for 16% of the total unclassified IT budget.

2. During the hearing, Rep. Andrew Clyde asked you to provide an estimate of the resources required of the agency to put together the data feeding into this Scorecard. In providing the Committee with that response, please provide as much information as possible relative to the time, money, and staff it takes to collect and assemble the data for DoD's data submissions for the Scorecard.

The IT Portfolio Management office feeds data into this Scorecard. The main focus of this office includes implementing a data-driven portfolio management approach that will improve the Department's IT decision-making process. At this time, we are not tracking the resources required to assemble the data that we would with a congressional reporting requirement.

3. Are there categories not included in the Scorecard that could or should be added to better measure DoD's information technology and cybersecurity posture?

DoD CIO recommends that the Committee on Oversight and Reform explore the possibility of using a cybersecurity scorecard, such as the DoD's cybersecurity scorecard, to assess an agency's cybersecurity posture and risk.